IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TENNESSEE

TRINA CROFT and HOWARD MATHIS, individually and on behalf of all others similarly situated, Plaintiffs, v. QRS, INC., a Tennessee corporation, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Trina Croft and Howard Mathis ("Plaintiffs") bring this Class Action Complaint against QRS, Inc. ("QRS" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard sensitive information that patients of Defendant's customers entrusted to it, including, without limitation, names, Social Security numbers, dates of birth, patient numbers, patient portal usernames, and/or addresses (collectively, "personally identifiable information" or "PII") as well as medical treatment and diagnosis information and/or personal health information (collectively, "protected health information" or "PHI"),[1] for failing to comply with industry standards to protect information systems that contain that PII and PHI, and for failing to provide

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PII and PHI had been accessed and potentially acquired by an unauthorized third party. Plaintiffs also allege that Defendant failed to provide timely, accurate, and adequate notice to Plaintiffs and Class Members regarding precisely what types of information was unencrypted and in the possession of unknown third parties. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members, and to provide a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes as Plaintiffs and Class Members will forever be at an increased risk of identity theft due to the conduct of QRS as described herein.

2. According to its website, QRS is a health care technology and services company with over twenty-five years of experience "providing physician's offices with practice management ("PM") and electronic records solutions ("EHR")."[2] For its customers, QRS offers services to assist with: "scheduling, charting, imaging, billing, patient engagement, encounter documentation, ***data security***, and more."[3] In relation to these services, Defendant operates a network system that contains electronic health records ("EHR"), stores health information, and stores confidential, personal information. QRS's customers include health care providers, medical service providers, and physicians "across America."[4]

3. In the ordinary course of receiving care from or doing business with Defendant's

[2] https://www.qrshs.com/ (last visited Jan. 11, 2022).
[3] *Id.*; https://www.qrshs.com/about (last visited Jan. 11, 2022) (emphasis added).
[4] https://www.qrshs.com/about (last visited Jan. 11, 2022).

customers, individuals such as Plaintiffs are regularly required to provide their PII and PHI to either Defendant QRS's customers or QRS directly by uploading it to QRS's patient portal.

4. Patient PII and PHI is then stored on Defendant's network system on its servers in Knoxville, Tennessee and backed up to what Defendant refers to as a "second offsite secure server location."[5]

5. From approximately August 23 to August 26, 2021, Defendant's internal administrative system experienced an external system breach or hacking by an "unknown, unauthorized third-party" (the "Data Breach").[6]

6. From approximately August 23 to August 26, 2021, this unauthorized third party accessed the server associated with Defendant's patient portal. The files on this server contained PII and PHI, which the unauthorized third party accessed and "may have acquired."[7]

7. During the Data Breach, the unauthorized third party accessed and potentially acquired the PII and PHI of more than 319,778 individuals which was being stored and maintained by Defendant.[8]

8. Before or on August 26, 2021, Defendant discovered the Data Breach. After taking the server containing the patient portal offline and initiating an investigation, Defendant finally began to alert health care providers of the Data Breach on or around September 7, 2021. Defendant provided these health care providers with an "update" regarding the Data Breach on October 1, 2021.[9]

9. On October 22, 2021, Defendant notified the U.S. Secretary of Health and Human

[5] QRS, *Disaster Recovery,* https://www.qrshs.com/disaster-recovery/ (last visited November 11, 2021).
[6] Ex. 1 (sample *Notice of Data Breach* filed with Massachusetts Attorney General).
[7] *Id.*
[8] DEPARTMENT OF HEALTH AND HUMAN SERVICES, Office for Civil Rights, Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited November 11, 2021).
[9] Ex. 1 at 1.

Services at the Office for Civil Rights ("HHS") of the Data Breach.[10] Also on or around that date, Defendant notified the Massachusetts State Attorney General.

10. Around the same time, Defendant finally began notifying Plaintiffs and Class Members of the Data Breach.

11. This case involves a breach of a computer system by an unknown third party, resulting in the unauthorized disclosure and potential acquisition of the PII and PHI of Plaintiffs and Class Members to unknown third parties. As a result of Defendant's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII and PHI was accessed and/or acquired and is now in the hands of criminals. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to QRS's failures.

12. Additionally, as a result of Defendant's failure to follow contractually agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs and Class Members received only a diminished value of the services Defendant was to provide.

13. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

14. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and/or specific, sensitive medical

[10] DEPARTMENT OF HEALTH AND HUMAN SERVICES, Office for Civil Rights, Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited November 11, 2021).

information.

15. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members. Defendant waited months to initially report the Data Breach to Plaintiffs and Class Members and still maintains secret the specific vulnerabilities and root causes of the Data Breach. Plaintiffs and Class Members remain unaware of precisely what information was unencrypted and now in the possession of unknown third parties.

16. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to adequately protect the PII and PHI of Plaintiffs and Class Members and warn Plaintiffs and Class Members of Defendant's inadequate information security practices. Defendant's conduct amounts to negligence and violates federal and state statutes.

17. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and, significantly (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

18. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

19. Plaintiff Trina Croft is a citizen of Florida residing in Union County, Florida.

20. Plaintiff Howard Mathis is a citizen of Florida residing in Columbia County, Florida.

21. Defendant QRS, Inc. is a for-profit corporation incorporated in the state of Tennessee, headquartered at 2010 Castaic Lane, Knoxville, Tennessee 37932, with its principal place of business in Knoxville, Tennessee.[11]

22. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of suchother responsible parties when their identities become known.

23. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

25. The Eastern District of Tennessee has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial

[11] https://tnbear.tn.gov/Ecommerce/FilingDetail.aspx?CN=1030891801400021891230690321890230912441261180 89 (last visited November 9, 2021).

business in Tennessee and this District through its headquarters, offices, parents, and affiliates.

26. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

27. Defendant is a health care technology and services corporation that provides software, billing, and physician management services for physicians and other health care providers ("providers" or "Defendant's customers"). According to Defendant's website "[QRS's] goal is to unburden [providers] from the technical and administrative responsibilities of managing [a] practice, so you can focus on what matters most—caring for your patients and growing your business."[12]

28. Defendant's software is used by "providers across America" to streamline "scheduling, charting, imaging, billing, patient engagement, encounter documentation, ***data security***, and more."[13] In relation to these services, Defendant operates a network system that contains Electronic Health Records ("EHR"), stores confidential health information, and confidential personal information.

29. For example, QRS's keystone software product PARADIGM offers its customers Practice Management and EHR services. According to Defendant's website,

> PARADIGM was designed as a single product with all the benefits of an EHR and Practice Management system. It is not a cobbled together system built from systems that were acquired by purchasing other companies. PARADIGM shares a single database between the EHR and the Practice Management system.

[12] https://www.qrshs.com/about (last visited November 11, 2021)
[13] *Id.*

This means you will never have to enter data twice."[14]

30. Defendant encourages its customers to use its services and technology, including PARADIGM EHR, to go "paperless" by uploading any and all patient records into an "electronic chart" stored and maintained by Defendant.[15] According to Defendant:

> PARADIGM EHR is our premium easy to use Electronic Health Records software product. PARADIGM EHR integrates scanning, electronic documents, note generation and work flow all into one system. This allows you to fully automate your charts completely eliminating the need for paper copies. PARADIGM EHR allows you to store virtually any type of file securely and quickly in a patient's electronic chart.[16]

31. Defendant's customers can upload patient information to the patient portal on QRS's servers either through QRS's Client Portal or through QRS's software.

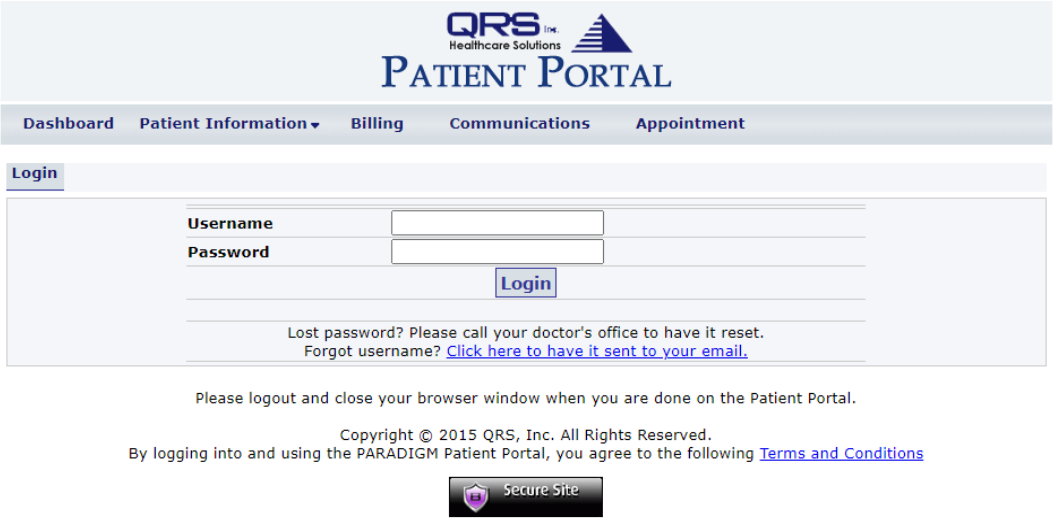
32. Additionally, patients can also access and upload their information directly through QRS's Patient Portal ("portal"). Patients can login to QRS's portal to access their patient information, add to or view their medical history, family history, social history, allergy information, insurance information, demographic information, and access their patient summary. Patients can also use the QRS Portal to schedule physician appointments and handle billing matters.[17]

33. The server subject to the Data Breach is associated with QRS's patient portal.

---

[14] https://www.qrshs.com/paradigm-pm/ (last visited November 11, 2021).
[15] http://www.qrshs.com/paradigm-ehr/# (last visited November 11, 2021).
[16] *Id.*
[17] *See* QRS Patient Portal Wayback Machine Access, dated Jan. 22, 2021, WAYBACK MACHINE INTERNET ARCHIVES, https://web.archive.org/web/20210122230429/https://portal.qrshs.com/index.php (last visited November 11, 2021) ("QRS Patient Portal Screenshot").

34. A screenshot of the appearance of the Patient Portal on January 21, 2021, is provided below.[18]



35. Defendant routinely acquires patient PII and PHI either directly from patients through the QRS Portal, or indirectly from Defendant's customers.

36. Defendant's customers are physicians, hospital systems, and other health care providers. Plaintiffs and Class Members are the patients of Defendant's customers. As a condition of receiving health care from Defendant's customers, Plaintiffs and Class Members were required to provide sensitive and confidential information to Defendant either directly, by using the QRS portal, or indirectly, through their respective health care providers.

37. Plaintiffs and the Class Members entrusted this sensitive and confidential information to Defendant to store and manage. This patient information included, without limitation, names, Social Security numbers, dates of birth, patient numbers, patient portal usernames, and/or addresses, as well as medical treatment and diagnosis information and other personal health information.

[18] *Id.*

38. The PII and PHI Defendant stores is sensitive and confidential. It includes medical treatment information and other PHI that may divulge underlying mental or physical diagnoses, as well as prescription, testing/laboratory results, physician's notes, and other personal health information contained in the patient's "electronic chart."

39. As recently as June 19, 2020, Defendant's website had a posted "Privacy Policy" ("Privacy Policy") meant to demonstrate its "firm commitment to your privacy and the protection of your information."[19] Within that Privacy Policy, Defendant stated that "[w]e use security measures to protect against the loss, misuse and alteration of data used by our system."[20] As of November 15, 2021, that Privacy Policy and the associated language is no longer listed on Defendant's website.[21]

40. Plaintiffs and Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

41. Defendant had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

42. On or about October 22, 2021, Defendant sent Plaintiffs and Class Members a form Notice of Data Incident.[22] that the Notice of Data Incident stated in part:

> **What Happened?** What Happened? On August 26, 2021, QRS discovered that an unknown, unauthorized third party accessed a

[19] Web Archive of Defendant's Privacy Policy on June 19, 2020), available at https://web.archive.org/web/20200619184724/http://qrshs.com:80/privacy-policy (last visited November 15, 2021).
[20] QRS Privacy Policy Wayback Machine Access, dated June 19, 2020, WAYBACK MACHINE INTERNET ARCHIVES https://web.archive.org/web/20200619184724/http://qrshs.com:80/privacy-policy (last visited November 15, 2021).
[21] https://www.qrshs.com/privacy-policy/ (last visited November 15, 2021).
[22] Ex. 1.

QRS server associated with our patient portal and may have acquired certain protected health information ("PHI") stored in the server.

Upon discovering the incident, we immediately took the server offline and began an investigation. We also engaged a forensic security firm to confirm the security of our network, analyze the incident, and determine the extent of the PHI that may have been accessed or acquired by the third party.

Our investigation has determined that the third party accessed the server from August 23, 2021, to August 26, 2021. During this time, the third party accessed, and may have acquired, files in the server that contained your PII. This incident did not involve any other QRS or «Variable Data 3» systems.

We provided an initial notification of the incident to «Variable Data 3» on September 7, 2021. Following additional investigation, we provided further notification of the incident to «Variable Data 3» on or about October 1, 2021. We have since been working with «Variable Data 3» to notify individuals as quickly as possible.

What Information Was Involved? Our investigation determined that the incident involved unauthorized access, and potentially unauthorized acquisition, of your personal information, including your name, Social Security number, date of birth, patient number, and portal username. The accessed or acquired information may have also contained an address and limited medical treatment or diagnosis information if it was uploaded to the QRS portal. At this time, we are not aware of any identity theft or fraud to any person as a result of this incident.

What We Are Doing. Data security is one of our highest priorities. As discussed above, upon discovering the incident, we immediately took the server offline, began an investigation, and engaged a forensic security firm to confirm the security of our network. We will keep this particular server offline permanently. We have taken steps to further secure our network and reduce the risk of a similar incident occurring in the future, including implementing multifactor authentication on core QRS systems for key administrators and implementing a Security Information and Event Management System (SIEM). QRS is also reviewing and updating its information security policies.

What You Can Do. Although we are not aware of any instances

> of fraud or identity theft involving your information, on behalf of «Variable Data 3» we are offering a complimentary two-year membership of Experian IdentityWorks™ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score.[23]

43. On or around October 22, 2021, Defendant reported the Data Breach to the U.S. Secretary of Health and Human Services at the Office for Civil Rights.[24] Also on or around that date, Defendant notified the Massachusetts State Attorney General of the Data Breach. Defendant provided the Massachusetts Attorney General with a "sample" notice of the Data Breach.[5]

44. Defendant admits in the Notice of Data Incident that an unknown, unauthorized third party accessed Defendant's server associated with its patient portal. Defendant also admits that an unauthorized third party accessed files containing sensitive information, including names, Social Security numbers, dates of birth, patient numbers, portal usernames, and, "if it was uploaded to QRS's portal," addresses and medical information, including "limited" medical treatment and diagnosis information.

45. Defendant has indicated that during the period of the Data Breach, the third party was not only able to access Plaintiffs' and Class Members' PII and PHI but was also able to acquire and/or remove that data from QRS's server.

46. Defendant claims that upon "discovering the incident, [Defendant] immediately took the server offline, began an investigation, and engaged a forensic security firm to confirm the

[23] Ex. 1 at 1. Upon Plaintiffs' information and belief, "<<Variable Data 3>>" represents the field in which the Defendant's customer name was later added for each individual notification letter to each respective patient.
[24] DEPARTMENT OF HEALTH AND HUMAN SERVICES, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information; *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited November 11, 2021).

security of [its] network."[25] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the adequacy of any remedial measures undertaken to ensure a breach does not occur again have not been transparently shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

47. The unencrypted PII and PHI of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members.

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained and stored belonging Plaintiffs and Class Members, causing the exposure of PII and PHI for more than 319,778 individuals.

The Health Care Sector is Particularly Susceptible to Data Breaches

49. Defendant was on notice that companies in the health care industry are targets for data breaches.

50. Defendant was also on notice that the FBI has been concerned about data security in the health care industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the health care industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting health care related systems, perhaps for the purpose of obtaining the Protected Health care Information (PHI) and/or Personally Identifiable Information (PII)."[26]

51. The American Medical Association ("AMA") has also warned health care companies about the importance of protecting their patients' confidential information:

[25] Ex. 1 at 1.
[26] Jim Finkle, *FBI Warns Health care Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-health care-fbi/fbi-warns-health care-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Jan. 11, 2022).

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[27]

52. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[28] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[29] That trend continues.

53. The health care sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[30] Indeed, when compromised, health care related data is among the most sensitive and personally consequential. A report focusing on health care breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[31] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling

---

[27] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Jan. 11, 2022).

[28] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/post/data-breaches-up-nearly-45-percent-according-to-annual-review-by-identity-theft-resource-center-and-cyberscout/(last visited Jan. 11, 2022).

[29] Identity Theft Resource Center, *Year-End Data Breach News Is a Grim Reminder: There's Work to Be Done , available at:* https://www.idtheftcenter.org/post/year-end-data-breach-news-is-a-grim-reminder-theres-work-to-be-done/ (last visited Jan. 11, 2022).

[30] Identity Theft Resource Center, *The 2018 Impact of Data Breaches and Cybercrime, available at*: https://www.idtheftcenter.org/post/2018-cybercrime-databreach-impact/ (last visited Jan. 11, 2022).

[31] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Jan. 11, 2022).

effect on individuals and detrimentally impact the economy as a whole.[32]

54. Health care related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[33] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[34]

Defendant Acquires, Collects, and Stores the PII and PHI of Plaintiffs and Class Members.

55. Defendant acquired, collected, and stored the PII and PHI of Plaintiffs and Class Members.

56. As a condition of using Defendant's customers' services or using Defendant's services, individuals entrusted Defendant with highly confidential PII and PHI.

57. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

58. Plaintiffs and Class Members have taken reasonable steps to maintain the

[32] *Id.*
[33] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Jan. 11, 2022).
[34] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Jan. 11, 2022).

confidentiality of their PII and PHI and implicitly relied on Defendant to keep their PII and PHI confidentialand securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

59. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendant could have mitigated the effects of the Data Breach by destroying data, especially outdated information.

60. Defendant's negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed toward protecting and securing sensitive data.

61. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

62. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiffs and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damageto victims may continue for years.

Value of Personal Identifiable Information

63. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[35] Experian reports that a stolen credit or

[35] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs/ (last visited

debit card number can sell for $5 to $110 on the dark web.[36] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

64. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety offraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security numbercan use it to get other personal information about you. Identity thieves can use your number and your good creditto apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment foritems you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

65. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number withoutsignificant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is notpermitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[37]

Jan. 11, 2022).

[36] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask- experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark- web/ (last visited Jan. 11, 2022).

[37] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-

67. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, Social Security numbers, medical records, and potentially date of birth.

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[38]

69. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

70. The PII and PHI of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

71. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future

about-identity-theft (last visited Jan 11, 2022).

[38] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 11, 2022).

harm.[39]

72. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

73. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

74. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. To date, Defendant has offered Plaintiffs and Class Members only two years of identity protection services through Experian Creditworks™ 3B. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

76. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

QRS's Conduct Violates HIPAA

77. Title II of HIPAA contains what are known as the Administrative Simplification

[39] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 11, 2022).

provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

78. Defendant is aware of the existence of HIPAA's Security Standards, and expressly refers to HIPAA's Security Standards (e.g., 45 CFR § 164.308(a)(i)) on its website.[40]

79. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII and PHI.

80. In addition, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and/or PHI when it was no longer necessary and/or had honored its customer's obligations to patients.

81. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information QRS creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

[40] https://www.qrshs.com/disaster-recovery/ (last visited November 11, 2021).

to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*; and

k. Retaining information past a recognized purpose and not deleting it.

82. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay

and ***in no case later than 60 days following discovery of the breach***."[41]

83. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

QRS Failed to Comply with FTC Guidelines

84. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

85. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[42]

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[43] The guidelines

[41] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 11, 2022).
[42] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. Jan. 11, 2022).
[43] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last

note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

87. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[44]

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Defendant was at all times fully aware of its obligation to protect the PII and PHI of patients because of its position as a software vendor for health care organizations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

visited Jan. 11, 2022).

[44] FTC, *Start With Security*, *supra*.

Plaintiff Trina Croft's Experience

91. Beginning in approximately 1986, Plaintiff Croft has been a patient of North Florida Eyecare, a customer of Defendant. As a condition of receiving services from North Florida EyeCare Plaintiff Croft was required to provide her PII and PHI.

92. Plaintiff received Defendant's Notice of Data Incident, dated October 22, 2021, on or about that date.[45] The notice stated that Plaintiff's name and Social Security number were contained in files accessed and potentially acquired during the Data Breach. The letter appeared in substantially the same form as the sample notice submitted to the Attorney General of Massachusetts.

93. As a result of the Notice of Data Incident, Plaintiff Croft spent time dealing witht h e consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Incident and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

94. Additionally, Plaintiff is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

95. Plaintiff stores any documents containing her sensitive PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

96. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI —a form of intangible property that Plaintiff entrusted Defendant for the purpose of health care treatment, which was compromised in and as a result of the Data Breach.

[45] Ex. 3 (Plaintiff's *Notice of Data Breach Letter*).

97. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

98. Plaintiff has suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and possibly criminals.

99. Plaintiff has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Howard Mathis's Experience

100. From approximately 2016 to approximately 2018, Plaintiff Mathis visited North Florida Eyecare, a customer of Defendant, to receive medical care. As a condition of receiving medical services, Plaintiff Mathis was required to provide his PII and PHI.

101. At the time of the Data Breach (August 23, 2021 to August 26, 2021), Defendant retained the names, Social Security numbers, and PHI of Plaintiff and other individuals in its internal, administrative system.

102. Plaintiff received Defendant's Notice of Data Incident, dated October 22, 2021, on or about that date. The notice stated that Plaintiff's name and Social Security number were contained in files accessed and potentially acquired during the Data Breach. The letter appeared in substantially the same form as the sample notice submitted to the Attorney General of Massachusetts.

103. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the

Notice of Data Incident and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

104. Additionally, Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

105. Plaintiff stores any documents containing his sensitive PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

106. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI —a form of intangible property that Plaintiff entrusted to Defendant for the purpose of health care treatment, which was compromised in and as a result of the Data Breach.

107. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss ofhis privacy.

108. Plaintiff has suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and possibly criminals.

109. Plaintiff has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

110. Plaintiffs bring this Class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil

Procedure.

111. The Class that Plaintiffs seek to represent is defined as follows:

> **All United States residents whose PII and/or PHI was actually or potentially compromised in the Data Breach reported by QRS, Inc. on or about October 22, 2021 (the "Class").**

112. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

113. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

114. Numerosity, Fed R. Civ. P. 23(a)(1): The Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals whose PII and PHI may have been improperly accessed and potentially acquired in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the Department of Health and Human Services that the Data Breach affected 319,778 individuals.

115. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of

Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

116. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

117. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class asa whole. Defendant's policies challenged herein apply to and affect Class Membersuniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

118. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiffs has retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action

vigorously.

119. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fairand efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against largecorporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and imposea burden on the courts.

120. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costsof individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicativeof this litigation.

121. The litigation of the claims brought herein is manageable. Defendant'suniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

122. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

123. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

124. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

125. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, andsafeguarding their PII and PHI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and

Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Plaintiffs and Class Members are third party beneficiaries of contracts between Defendant and health care providers which collected PII and PHI from Plaintiffs and Class Members;

g. Whether Defendant breached the contracts with health care providers of which Plaintiffs and Class Members are third party beneficiaries;

h. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

126. Plaintiffs and Class Members re-allege and incorporate by reference herein all of the previous allegations.

127. In the course of using Defendant's services and/or receiving care from Defendant's customers, Plaintiffs and Class Members were obligated to provide their PII and PHI to either QRS directly or to QRS's customers.

128. Plaintiffs and Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

129. Defendant has full knowledge that the PII and PHI belonging to Plaintiffs and Class Members contained personal and sensitive medical information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms and the types of harm that Plaintiffs and the Class Members could and would suffer if the PII and PHI were wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

130. Defendant knew or reasonably should have known that the failure to exercise due care in collecting, storing, and using Plaintiffs' and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiffs and the Class.

131. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendant's possession was adequately secured and protected.

132. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patient's PII and PHI it was no longer permitted to retain pursuant to regulations.

133. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII and PHI.

134. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiffs and Class Members That relationship

arose because Plaintiffs and the Class Members entrusted Defendant with their confidential PII and PHI, a necessary part receiving care from Defendant's customers and/or using Defendant's services.

135. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

136. Defendant had a common law duty to prevent foreseeable harm to those whose PII it stored. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices.

137. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

138. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiffs and Class Members' PII and PHI, the critical importance of providing adequate security, and the necessity of encrypting PII and PHI stored on Defendant's systems. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by Defendant's failure to protect their PII and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, QRS knew or should have known that it was more likely than not Plaintiffs and Class Members would be harmed.

139. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII and PHI, including basic encryption techniques easily available to Defendant.

140. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in,

and possibly remains in, Defendant's possession.

141. Defendant and only Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

142. Defendant had and continues to have a duty to accurately and adequately disclose details of the Data Breach. This information is necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

143. Defendant has admitted that the PII and PHI of Plaintiffs and the Class was wrongfully disclosed and/or lost to unauthorized third persons as a result of the Data Breach.

144. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

145. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and Class Members in the face of increased risk of theft.

146. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and the Class Members' PII and PHI.

147. Defendant's failure to comply with industry and federal regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII and PHI.

148. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data

Breach.

149. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

150. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered. The PII and PHI of Plaintiffs and the Class was accessed and/or lost as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

151. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

152. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

153. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

154. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

155. Defendant's violations of HIPAA also constitute negligence *per se*.

156. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' health care information and set forth the conditions under which such

information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to health care providers and the organizations they work for, but to any entity that may have access to health care information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

157. Plaintiffs and the Class are within the class of persons that HIPAA privacy laws were intended to protect.

158. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

159. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI are used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

160. As a direct and proximate result of Defendant's negligence and negligence *per se* Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

161. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

162. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs and the Class re-allege and incorporate by reference herein all of the previous allegations.

164. As a condition of using Defendant's services and/or receiving care from Defendant's customers, Plaintiffs and Class Members were obligated to provide their PII and PHI to either QRS directly or to Defendant QRS's customers.

165. As a condition of these services, Plaintiffs and Class Members provided their PII to Defendant directly or to Defendant's customers. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached, compromised or stolen.

166. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

167. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data and cyber security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Defendant would use part of the monies paid to Defendant either by them directly or through Defendant's customers, to fund adequate and reasonable data and cyber security practices.

168. Plaintiffs and Class Members would not have provided and entrusted their health-related information to Defendant or Defendant's customers in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of Plaintiffs' and Class Members' PII and PHI was critical to realize the intent of the parties.

169. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that their personal information was compromised as a result of the Data Breach.

170. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost

work time; and other economic and non-economic harm.

171. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

172. Plaintiffs and the Class re-allege and incorporate by reference herein all of the previous allegations.

173. Plaintiffs and Class Members had a legitimate expectation of privacy with regard to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

174. Defendant owed a duty to those individuals whose PII Defendant collected and stored as part of its services rendered to keep their PII and PHI obtained as a condition thereof, confidential.

175. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Class.

176. Defendant allowed unauthorized and unknown third parties access to Plaintiffs' and Class Members' PII and PHI.

177. The unauthorized release of highly sensitive, confidential personal information such as an individual's Social Security number to unauthorized third parties is highly offensive to a reasonable person.

178. Plaintiffs' and Class Members' PII and PHI are private and are entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of their relationships with

Defendant and/or Defendant's customers, but with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

179. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the e Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

180. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it acted with actual knowledge that its information security practices were inadequate and insufficient.

181. Defendant had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

182. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiffs and the Class were disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

183. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

184. As a direct and proximate result of Defendant's invasion of privacy, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

185. Plaintiffs and the Class re-allege and incorporate by reference herein all of the previous allegations.

186. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of their PII and PHI, which Plaintiffs and Class Members provided to Defendant and/or Defendant's customers in confidence.

187. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class was governed by terms and expectations that Plaintiffs' and Class Members' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

188. Plaintiffs and Class Members provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

189. Plaintiffs and the Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

190. Defendant received in confidence Plaintiffs' and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

191. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties without their express permission.

192. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Class have suffered damages.

193. But for Defendant's disclosure of Plaintiffs' and Class Members' PII and PHI in violation of the parties' understanding of confidence, their private information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

194. The injury and harm Plaintiffs and the Class suffered were the reasonably foreseeable results of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing the PII and PHI of Plaintiffs and Class Members.

195. As a direct and proximate result of Defendant's breach of confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI are used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that PII and PHI; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair

the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

196. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class are entitled to recover actual, consequential, andnominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and their Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and the Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of PII and PHI;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and the Class;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

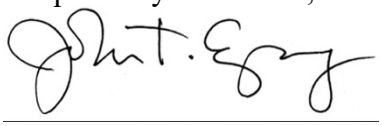
G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 19, 2022

Respectfully Submitted,



John Spragens, TN BPR No. 31445
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: 615-983-8900
F: 615-682-8533
john@spragenslaw.com

Jean S. Martin*
Francesca Kester*
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice applications forthcoming*